

REMARKS

Claims 1-21 are pending. Claim 1 is the only independent claim and has been amended. Favorable reconsideration is respectfully requested.

Claims 1-16 and 19-21 were rejected under 35 U.S.C. § 103 over U.S. Patent 7,350,076 (Young et al.) in view of U.S. Patent Publication 2004/0103283 (Hornak). Claims 17 and 18 were rejected under 5 U.S.C. § 103 over Young et al. and Hornak, and further in view of U.S. Patent 5,515,439 (Bantz et al.). Applicants submit that amended independent claim 1 is patentable over the cited art for at least the following reasons.

Amended claim 1 relates to a method for the secure access of a mobile terminal to a Wireless Local Area Network (WLAN) and for secure data communication via wireless link. In the method, when a Mobile Terminal (MT) logs on a wireless Access Point (AP), the Mobile Terminal (MT) and the Access Point (AP) execute a two-way certificate authentication wherein a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS). Then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned from the Authentication Server (AS) to the Access Point (AP) and the Mobile Terminal (MT) so that the Access Point (AP) obtains the authentication result of the Mobile Terminal (MT) and the Mobile Terminal (MT) obtains the authentication result of the Access Point (AP). Further, the Mobile Terminal (MT) and the Access Point (AP) perform negotiation of secret key for conversation.

The Office Action conceded that Young et al. failed to teach the limitation relating to the transmission to, and authentication by, the AS of the MT certificate and AP when a Mobile Terminal logs on. However, the position was taken that this feature was taught in Hornak. Applicants disagree.

In the Response After Final Office Action filed June 22, 2010, it was stated, at page 14, that unlike Hornak, "claim 1 solves this problem and achieves real-time authentication of the certificates not only regarding formality, but also validity when they are in use." In the Advisory

Action mailed July 2, 2010, the Examiner stated that this is not sufficiently found in the claim language. Applicants disagree.

Claim 1 recites, inter alia, that “when a Mobile Terminal (MT) logs on a wireless Access Point (AP), the Mobile Terminal (MT) and the Access Point (AP) execute a two-way certificate authentication wherein a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS).”

One skilled in the art knows that the Authentication Server in the technical field of secure telecommunication has the independent function for issuance and management of the certificates. Since such certificates of the MT and AP are previously issued by the Authentication Server when these certificates are in use, if they are returned back to the authentication server for authentication, the person skilled in the art would recognize that not only the formality but also the validity of the certificates will be verified by the Authentication Server. Thus, it is now believed even more clear that the invention of claim 1 makes inventive use of this characteristic of the authentication server to achieve real time authentication of the certificates *not only regarding formality but also validity* when they are in use.

In fact, at this point, the Authentication Server is already involved in the two way authentication between the MT and AP. One skilled in the art would know that without the authentication server, neither the MT nor the AP has the independent ability for authenticating the validation of the other party's certificate. Therefore, the feature “a Mobile Terminal (MT) certificate and an Access Point (AP) certificate are transmitted to an Authentication Server (AS) and are authenticated through the Authentication Server (AS)” itself indicates that both the formality and validity of the certificates are authenticated.

As mentioned above, the Authentication Server in the technical field of secure telecommunication has the independent function for issuance and management of the certificates. Hornak's paragraph [0083], cited in the Office Action, relates to the function of *certificates*

issuance of the certification authority (CA) 48, as opposed to its certificate authentication function. Paragraph [0083] does mention, as the examiner noted, that “the CA 48 is accessible by the client 42, the origin server 44 and the gateway 46 for authentication of a certificate belonging to each of these parties.” However, applicants submit that from the context of Hornak, especially from the corresponding interpretation of the subsequent paragraphs, it can be seen that “authentication” as discussed in paragraph [0083] *relates to the issuance stage only*.

The feature of claim 1 “then the authentication result of the Mobile Terminal (MT) certificate and the Access Point (AP) certificate is returned from the Authentication Server (AS) to the Access Point (AP) and the Mobile Terminal (MT) so that the Access Point obtains the authentication result of the Mobile Terminal and the Mobile Terminal obtains the authentication result of the Access Point” make the difference even more clear. It can be seen that the authentication result here includes those obtained by authenticating the certificates of both the MT and AP. In this way, the MT is informed of the status of the AP’s certificate and the AP is informed of that of the MT’s certificate and two-way certificate authentication between MT and AP is achieved by the involvement of the Authentication Server.

Furthermore, according to claim 1, upon a condition that the authentication result is returned to AP and MT by AS, when the Access Point obtains the authentication result of the Mobile Terminal and the Mobile Terminal obtains the authentication result of the Access Point, authentication between AP and MT finishes.

In contrast, in Hornak, as the Examiner correctly mentioned towards the end of the comments in the Continuation Sheet of the Advisory Action, “upon successful authentication occurring, another authentication procedure commences between the two entities separately.” Particularly, in Hornak, when the gateway or client has its certificate signed by the CA and receives its own certificate with CA signature, Hornak refers to this as the gateway or client having been successfully authenticated *personally*. Therefore, in Hornak, only the authentication result of the Gateway (which can be seen to correspond to the AP) certificate is returned to the Gateway while

the authentication result of the client certificate (which can be seen to correspond to the MT) is returned to the client (please refer to [0084] of Hornak).

Thus, at this stage, to show the other parties that they have been personally identified by the CA (see, e.g., paragraph [0084] of Hornak), authentication between the gateway and the client is necessary. Therefore, in Hornak, a further step that the gateway and the client verify the signed certificate of each other, called a protocol handshake, is needed (see, e.g., paragraph [0110] and FIG. 5 of Hornak).

Thus, procedurally, it can be seen that in claim 1, when the authentication result is returned by AS, the authentication between AP and MT is completed. In contrast, in Hornak, only personal authentication has been completed at the corresponding stage, while authentication between AP and MT has not yet started.

For at least the foregoing reasons, claim 1 is believed clearly patentable over the cited references. This is particularly true when the recited claim elements are taken as a whole in combination, rather than examined individually out of context.

The dependent claims are believed patentable for at least the same reasons as claim 1. The other references are not believed to remedy the abovementioned deficiencies of the cite art.

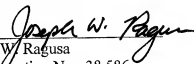
In view of the above amendments and remarks, applicants believe the pending application is in condition for allowance.

REQUEST FOR INTERVIEW

Applicants request that before issuance of the next Office Action, the Examiner telephone applicants' undersigned representative to set up a mutually convenient time for a telephone interview to move this case closer to allowance.

Dated: July 22, 2010

Respectfully submitted,

By 
Joseph W. Ragusa
Registration No.: 38,586
DICKSTEIN SHAPIRO LLP
1633 Broadway
New York, New York 10019-6708
(212) 277-6500
Attorney for Applicant